Max-Clique

Largest subset of vertices with all edges present
Max-Clique

Largest subset of vertices with all edges present

Clique(G) = 5
Max-Clique

Complexity?
Complexity of Max-Clique

NP-Hard: made Karp’s list.

NP-Hard to approximate in $n^{1-\epsilon}$ (Hastad 99, Zuckerman 06).

Unconditional?
Unconditional Lower Bounds

Monotone Circuits: Razborov 85

SDP Hierarchies: Tulsiani 09

Average-Case?
Average-Case Complexity

Model: Erdös-Renyi Graphs

Each edge present with probability $1/2$
Average-Case Complexity

Max-Clique $\sim 2 \log_2 n$

Each edge present with probability $1/2$
Average-Case Complexity

Easy to find cliques of size $\log_2 n$

Each edge present with probability $1/2$
Average-Case Complexity

Challenge (Karp 76): Find clique of size \((1+\epsilon)\log_2 n\)?

Each edge present with probability \(1/2\)
Planted Clique

Jerrum, Kucera (92, 95): For what $t$ can we find the clique?

Each edge present with probability $1/2$
Planted Clique

Best - AKN98: Can do $t = n^{1/2}$ efficiently.

$G(n,1/2) + \text{Clique}(t)$

Each edge present with probability $1/2$
Why?
Natural algorithmic problem and test bed:
Spectral, Community detection, …
Natural algorithmic problem and test bed:
Spectral, Community detection, …

Natural average-case hardness assumption:
Cryptosystems [Juels, Peinado 01]
Nash Equilibria [Hazan, Krauthgamer 11]
Sparse PCA [Berthet, Rigollet 13]
Natural average-case hardness assumption:
- Cryptosystems [Juels, Peinado 01]
- Nash Equilibria [Hazan, Krauthgamer 11]
- Sparse PCA [Berthet, Rigollet 13]
Natural average-case hardness assumption:

Cryptosystems [Juels, Peinado 01]
Nash Equilibria [Hazan, Krauthgamer 11]
Sparse PCA [Berthet, Rigollet 13]
Square-Root Barrier

- Jerrum 92: Can’t do $o(n^{1/2})$ using MCMC algorithms.

- Feige, Krauthgamer 00, 03: Using $LS_+(r)$
  - Can only if planted-clique = $\Theta(\sqrt{n}/2^r)$.

- FGRVX 13: Can’t do* $o(n^{1/2})$ using statistical algorithms.
Main: Sum-of-Squares of r rounds cannot find cliques of size $\sim n^{1/2r}$.

Polynomial time $\sim r=O(1)$: Can’t handle $n^{o(1)}$.

**Strongest Optimization framework we have:**
- [BBHKSZ12] Solves Khot-Vishnoi gap instances
- [BRS11, GS11]: Sub-exponential for unique games

[LRS 14]: Captures many semi-definite programs.
Motivation

Results

Association Schemes

Locally Random Matrices

Sum-of-Squares

Proof Outline
Motivation

Results

Association Schemes

Locally Random Matrices

Sum-of-Squares Proof Outline
Tool 1: Johnson Scheme

\[ \mu : \{0, \ldots, r\} \rightarrow \mathbb{R} \]

\[ M_{\mu} \]

\[ \mu(|I \cap J|) \]

\[ \binom{n}{r} \]
Tool 1: Johnson Scheme

Given $\mu$ what can we say about the matrix?

$\mu : \{0, \ldots, r\} \rightarrow \mathbb{R}$
Tool 1: Johnson Scheme

Everything!

All matrices commute.

$\mu : \{0, \ldots, r\} \rightarrow \mathbb{R}$

$M_\mu$
Tool 1: Johnson Scheme

\[ \mu \Rightarrow \text{Eigenspaces, eigenvalues.} \]

“Fourier transform”.

\[ \mu : \{0, \ldots, r\} \rightarrow \mathbb{R} \]

\[ M_\mu \]
Tool 1: Johnson Scheme

Which matrices are PSD?
Ex: Faster than geometric decay $\Rightarrow$ PSD.

$\mu : \{0, \ldots, r\} \rightarrow \mathbb{R}$
Tool 2: Locally Random Matrices
Random Matrices 101
Random Matrices 101

Spectral gap of random \(\{0, 1\}\) matrix: \(O(n^{1/2})\).
Random Matrices/Graphs 101

Spectral gap of random \( \{0, 1\} \) matrix: \( O(n^{1/2}) \).

Spectral gap of random graph: \( O(n^{1/2}) \).

\[
\begin{bmatrix}
0 & 0 & 1 & 1 & 0 & 0 \\
0 & 0 & 1 & 1 & 0 & 0 \\
0 & 1 & 0 & 0 & 1 & 0 \\
0 & 1 & 1 & 1 & 1 & 0 \\
0 & 1 & 0 & 0 & 1 & 0 \\
1 & 1 & 0 & 0 & 1 & 1
\end{bmatrix}
\]

\( G(n, 1/2) \)
Random Matrices/Graphs 101

Spectrum?

G(n, 1/2)

Higher order incidences?

\[
\begin{array}{cccccc}
0 & 0 & 1 & 1 & 0 & 0 \\
0 & 0 & 1 & 1 & 0 & 0 \\
0 & 1 & 0 & 0 & 1 & 0 \\
0 & 1 & 1 & 1 & 1 & 0 \\
0 & 1 & 0 & 0 & 1 & 0 \\
1 & 1 & 0 & 0 & 1 & 1 \\
\end{array}
\]
Locally Random Matrices

\[ G(n, 1/2) \]

\[
\begin{pmatrix}
\binom{n}{r}
\end{pmatrix}
\]
Locally Random Matrices

$G(n, 1/2)$

Local function

$\binom{n}{r}$

$\binom{[n]}{r}$
Locally Random Matrices

$M(I,J)$: function of edges in $I \cup J$. 

$G(n,1/2)$

Local function

$f(G(I \cup J))$
Locally Random Matrices

Example: Number of edges in sub-graph; Is \( I \cup J \) a clique?

\[
G(n, 1/2) \quad \binom{[n]}{r} \quad J
\]

Local function \( f(G(I \cup J)) \)
Locally Random Matrices

Spectrum? Dependent entries ...

$G(n, 1/2)$

Local function $I$

$J$

$f(G(I \cup J))$
Norms of Locally Random Matrices

M: locally random matrix with 0 expectation.
Goal: Bound norm of M?

Trace method: Estimate $E[Tr(M^q)]$ and use

$$\|M\| \leq Tr(M^q)^{1/q}.$$ 

Core Lemma: Combinatorial tools to make trace calculations easy for locally random matrices.
Norms of Locally Random Matrices

Lemma: $M(I,J) \sim \text{Is } I \times J \text{ a bipartite clique?}$

Then, $\|M\| = \tilde{O}(n^{r-0.5}).$

Core Lemma: Combinatorial tools to make trace calculations easy for locally random matrices.
Norms of Locally Random Matrices

Lemma: $M(I,J) \sim \text{Is } I \times J \text{ a bipartite clique?}$

Then, $\|M\| = \tilde{O}(n^{r-0.5})$.

(Shifted to have zero mean).

Core Lemma: Combinatorial tools to make trace calculations easy for locally random matrices.
Motivation

Results

Association Schemes

Locally-Random Matrices

Sum-of-Squares

Proof Outline
Motivation

Association Schemes

Results

Locally-Random Matrices

Sum-of-Squares Proof Outline
Motivation

Results

Association Schemes

Locally-Random Matrices

T Prover 1000x

Sum-of-Squares

Proof Outline
Lasserre Hierarchy

= Sum-of-Squares Hierarchy

= Positivstellensatz Proof Systems
Lasserre Hierarchy
= Sum-of-Squares Hierarchy
= Positivstellensatz Proof Systems
Nullstellensatz [Hilbert]

When is a system of polynomial equations feasible?
Nullstellensatz [Hilbert]

\[ f_1, \ldots, f_m \in \mathbb{C}[x_1, x_2, \ldots, x_n] \]

\[
\begin{align*}
    f_1(x) &= 0 \\
    \vdots & \\
    f_m(x) &= 0
\end{align*}
\]

\[ \exists g_1, \ldots, g_m \] \[ \sum_i f_i g_i = 1 \]

The ‘Fundamental’ theorem of algebra
Positivstellensatz

\[ f_1, \ldots, f_m \in \mathbb{R}[x_1, x_2, \ldots, x_n] \]

\[
f_1(x) = 0 \\
\vdots \\
f_m(x) = 0
\]

Infeasible iff

\[
\exists g_1, \ldots, g_m \\
\sum_i f_i g_i = 1
\]

Ex: \( x^2 + 1 = 0 \).
Positivstellensatz

\[ f_1, \ldots, f_m \in \mathbb{R}[x_1, x_2, \ldots, x_n] \]

\[ f_1(x) = 0 \]
\[ \vdots \]
\[ f_m(x) = 0 \]

Infeasible \iff

\[ \exists g_i, h_j \]
\[ \sum_i f_i g_i = \frac{1}{1 + \sum_j h_j^2} \]

Real Algebraic Geometry
Positivstellensatz

\[ f_1, \ldots, f_m \in \mathbb{R}[x_1, x_2, \ldots, x_n] \]

\[ f_1(x) = 0 \]
\[ \vdots \]
\[ f_m(x) = 0 \]

Infeasible iff

\[ \exists g_i, h_j \]
\[ \sum_i f_i g_i = \frac{1}{1 + \sum_j h_j^2} \]

Not very useful for ‘proofs’: large degrees.
Positivstellensatz Proof System (GV01)

\[ f_1, \ldots, f_m \in \mathbb{R}[x_1, x_2, \ldots, x_n] \]

\[ f_1(x) = 0 \]
\[ \vdots \]
\[ f_m(x) = 0 \]

Refutation

Equivalent \sim \text{Lasserre}(r), \text{SOS}(r)

Degree

\[ \text{degree}(f_ig_i, h_j^2) \leq 2r \]

\[ \sum_i f_ig_i = 1 + \sum_j h_j^2 \]
Positivstellensatz Proof System (GV01)

\[ f_1, \ldots, f_m \in \mathbb{R}[x_1, x_2, \ldots, x_n] \]

\[
\begin{align*}
  f_1(x) &= 0 \\
  \vdots \\
  f_m(x) &= 0
\end{align*}
\]

PS(r) Refutation

Can find certificate in \( n^{O(r)} \) time.
Lasserre Lower bounds
= Sum-of-Squares Lower bounds
= No PS(r) Refutations
This Work

Main: Sum-of-Squares of $r$ rounds cannot find cliques of size $\sim n^{1/2r}$. 
This Work

Main: No PS(r) refutations for planted cliques of size $\sim n^{1/2r}$. 
Clique Axioms

Graph G. Max-Clique(G) > k?

\[ x_i^2 = x_i, \ i \in [n] \]

\[ x_i x_j = 0, \ \{i, j\} \notin G \]

\[ \sum_i x_i = k \]

Main: G ~ G(n,1/2). With high probability, no PS(r) refutation for k ~ n^{1/2r}.
Refuting Refutations: Duality

\[ f_1(x) = 0 \]
\[ \vdots \]
\[ f_m(x) = 0 \]

**PS(r) Refutation**

\[ \text{degree}(f_i g_i, h_j^2) \leq 2r \]
\[ \sum_i f_i g_i = 1 + \sum_j h_j^2 \]

**No PS(r) refutation iff** exists linear mapping \( M: \{ \text{degree 2r polynomials} \} \rightarrow \mathbb{R} \) such that:

1) \( M(f_i g_i) = 0, i \in [m] \)

2) \( M(h_j^2) \geq 0. \)
Refuting Refutations: Duality

\[ f_1(x) = 0 \]
\[ \vdots \]
\[ f_m(x) = 0 \]

PS(r) Refutation

No PS(r) refutation iff exists linear mapping \( M: \{\text{degree } 2r \text{ polynomials}\} \rightarrow \mathbb{R} \) such that:

1) \( M(f_i g_i) = 0, i \in [m] \)
2) \( M(h_j^2) \geq 0 \).

\[ \text{degree}(f_i g_i, h_j^2) \leq 2r \]

\[ \sum_i f_i g_i = 1 + \sum_j h_j^2 \]
Refuting Refutations: Duality

No PS(r) refutation iff exists linear mapping $M: \{\text{degree 2r polynomials}\} \rightarrow \mathbb{R}$ such that:

1) $M(f_ig_i) = 0, i \in [m]$  
2) $M(h_j^2) \geq 0$.  

“Semi-Definite”
Three step strategy

1. Linear algebra: Guess dual certificate $M$.

2. Prove $M$ is PSD
   a) Matrix analysis: $E[M]$ highly PSD
   b) Large deviation: Norm of $M-E[M]$ small.
Dual Certificate M

Graph G. Max-Clique(G) > k?

\[ M \left( \prod_{i \in I} X_i \right) = degree_G(I) \cdot \frac{k}{\binom{|I|}{2r}} \]
Dual Certificate $M$

Graph $G$. $\text{Max-Clique}(G) > k$?

\[ M \left( \prod_{i \in I} X_i \right) = degree_G(I) \cdot \frac{(k)}{\binom{|I|}{2r}} \]

“Normalization”
Dual Certificate $M$

Graph $G$. Max-Clique($G$) > $k$?

$$M \left( \prod_{i \in I} X_i \right) = \text{degree}_G(I) \cdot \frac{k}{|I|} \frac{|I|}{2r}$$

More interesting
Dual Certificate $M$

Graph $G$. Max-Clique($G$) $> k$?

$$M \left( \prod_{i \in I} X_i \right) = \text{degree}_G(I) \cdot \frac{k}{|I|} \cdot \frac{|I|}{2r}$$
Dual Certificate M

Graph G. Max-Clique(G) > k?

\[ M \left( \prod_{i \in I} X_i \right) = \deg_G(I) \cdot \frac{k}{|I|} \cdot \frac{2r}{|I|} \]
Dual Certificate M

Graph G. Max-Clique(G) > k?

\[ M \left( \prod_{i \in I} X_i \right) = \text{degree}_G(I) \cdot \frac{\binom{k}{|I|}}{\binom{2r}{|I|}} \]
Dual Certificate M

Graph G. Max-Clique(G) > k?

$$M \left( \prod_{i \in I} X_i \right) = degree_G(I) \cdot \left( \frac{k}{|I|} \right) \left( \frac{2r}{|I|} \right)$$
Dual Certificate M

Graph G. Max-Clique(G) > k?

\[ M \left( \prod_{i \in I} X_i \right) = \text{degree}_G(I) \cdot \frac{\binom{k}{|I|}}{\binom{2r}{|I|}} \]
Dual Certificate $M$

Graph $G$. Max-Clique($G$) > $k$?

\[
M \left( \prod_{i \in I} X_i \right) = \text{degree}_G(I) \cdot \frac{k}{|I| \choose 2r}
\]

$\text{degree}_G(I) = \text{No. of } 2r \text{ cliques containing } I.$

Ex: $I = \{v\}$, $r = 1$. $\text{degree}_G(I) = \text{deg}(v)$.
Positive Semi-Definiteness

\[ M \left( \prod_{i \in I} X_i \right) = \text{degree}_G(I) \cdot \frac{\binom{k}{|I|}}{2^r} \]

\[ \begin{array}{cccc}
\text{I} & & & \text{J} \\
& \ddots & & \\
& & \ddots & \\
& & & \text{M} \\
\end{array} \]

\[ \begin{pmatrix}
\binom{n}{r} \\
\binom{n}{r} \\
\end{pmatrix} \quad \begin{pmatrix}
M(I \cup J) \\
\geq 0?
\end{pmatrix} \]
Positive Semi-Definiteness

2. Prove $M$ is PSD
   a) Matrix analysis: $E[M]$ highly PSD
   b) Large deviation: Norm of $M - E[M]$ small.
Positive Semi-Definiteness

2. Prove M is PSD
   a) Matrix analysis: $E[M]$ highly PSD
      Tool 1: Johnson scheme.
   b) Large deviation: Norm of $M - E[M]$ small.
Positive Semi-Definiteness

2. Prove $M$ is PSD
   a) Matrix analysis: $E[M]$ highly PSD
   b) Large deviation: Norm of $M - E[M]$ small.

Tool 2: $M = \text{Locally-random + Error.}$
Positive Semi-Definiteness

Let us look at Special case:

\[ M(I, J) = deg_G(I, J) \]

Not local. Very high-variance.
Positive Semi-Definiteness

Let us look at Special case:

\[ M(I, J) = \deg_G(I, J) \]

\[ M(I, J) = E[\deg_G(I, J)] + L(I, J) + \Delta(I, J) \]
Positive Semi-Definiteness

Let us look at Special case:

\[ M(I, J) = \deg_G(I, J) \]

\[ M(I, J) = E[\deg_G(I, J)] + L(I, J) + \Delta(I, J) \]

\[ L(I, J) = \begin{cases} 
-E[\deg_G(I, J)] & \text{if } I \cup J \text{ not a clique} \\
\mu(|I \cup J|) & \text{otherwise} 
\end{cases} \]
Positive Semi-Definiteness

Let us look at Special case:

\[ M(I, J) = \deg_G(I, J) \]

\[ M(I, J) = E[\deg_G(I, J)] + L(I, J) + \Delta(I, J) \]

L is locally-random.
Positive Semi-Definiteness

Let us look at Special case:

\[ M(I, J) = \deg_G(I, J) \]

\[ M(I, J) = E[\deg_G(I, J)] + L(I, J) + \Delta(I, J) \]

\[ \Delta(I, J) = \begin{cases} 
0 & \text{if } I \cup J \text{ not a clique} \\
\deg_G(I, J) - E[\deg_G(I, J)] & \text{otherwise}
\end{cases} \]
Positive Semi-Definiteness

Let us look at Special case:

\[ M(I, J) = \text{deg}_G(I, J) \]

\[ M(I, J) = E[\text{deg}_G(I, J)] + L(I, J) + \Delta(I, J) \]

Lemma 1: Whp, \( ||L|| \sim n^{r-.5} \).

Lemma 2: Whp, \( ||\Delta|| \sim n^{r-.5} \).
Motivation

Results

Association Schemes

Locally-Random Matrices

Sum-of-Squares

Proof Outline
Open Problems

Can SOS beat $n^{1/2}$ in polynomial time?

[Kelner]: For $r=2$, our dual certificate fails at $k \sim n^{1/3}$!

Thank You